GitHub General Privacy Statement

In this article

GitHub Privacy Statement

Effective date: February 1, 2024

Welcome to the GitHub Privacy Statement. This is where we describe how we handle your “Personal Data”, which is information that is directly linked or can be linked to you. It applies to the Personal

Data that GitHub, Inc. or GitHub B.V., processes as the “Data Controller” when you interact with websites, applications, and services that display this Statement (collectively, “Services”). This Statement does not apply to services or products that do not display this Statement, such as Previews, where relevant.

End User Notice: Organization-Provided GitHub Accounts

When a school or employer supplies your GitHub account, they assume the role of Data Controller for most Personal Data used in our Services. This enables them to:

- Manage and administer your GitHub account, including adjusting privacy settings.
- Access and utilize your Personal Data, which includes details on how you use the Services, as well as your content and files.

Should you access a GitHub Service through an account provided by an organization, such as your employer or school, the organization becomes the Data Controller, and this Privacy Statement's direct applicability to you changes. Even so, GitHub remains dedicated to preserving your privacy rights. In such circumstances, GitHub functions as a Data Processor, adhering to the Data Controller's instructions regarding your Personal Data's processing. A Data Protection Agreement governs the relationship between GitHub and the Data Controller. For further details regarding their privacy practices, please refer to the privacy statement of the organization providing your account.

In cases where your organization grants access to GitHub products, GitHub acts as the Data Controller solely for specific processing activities. These activities are clearly defined in a contractual agreement with your organization, known as a Data Protection Agreement. You can review our standard Data Protection Agreement at GitHub Data Protection Agreement. For those limited purposes, this Statement governs the handling of your Personal Data. For all other aspects of GitHub product usage, your organization's policies apply.

Third Party Access and Data Protection

When you use third-party extensions, integrations, or follow references and links within our Services, the privacy policies of these third parties apply to any Personal Data you provide or consent to share with them. Their privacy statements will govern how this data is processed.

Personal Data We Collect

Personal Data is collected from you directly, automatically from your device, and also from third parties. The Personal Data GitHub processes when you use the Services depends on variables like how you interact with our Services (such as through web interfaces, desktop or mobile applications), the features you use (such as pull requests, Codespaces, or GitHub Copilot) and your method of accessing the Services (your preferred IDE). Below, we detail the information we collect through each of these channels:

From You

- Account Data: We collect certain information when you open an account such as your GitHub handle, name, email address, password, payment information and transaction information.
- User Content and Files: When you use our Services, we collect Personal Data included as part of the information you provide such as code, inputs, text, documents, images, or feedback.
- Demographic information: In some cases, you provide us with ethnicity, gender, or similar demographic details.
- Feedback Data: This consists of information you submit through surveys, reviews, or interactive features.
- Payment Information: For paid subscriptions, we collect details like name, billing address, and payment specifics.
- Profile Information: We collect information to create a user profile, which may include a photo, additional email addresses, job title, or biography.
- Sales and Marketing Data: This includes information provided for promotional communications, such as name, email address, and company name.
- Support Data: When you seek customer support, we collect details like code, text, or multimedia files.

Automatically

- Buttons, Tools, and Content from Other Companies: Our Services may contain links or buttons that lead to third-party services like Twitter or LinkedIn. Use of these features may result in data collection. Engaging with these buttons, tools, or content may automatically send certain browser information to these companies. Please review the privacy statements of these companies for more information.
- Essential Cookies and Similar Tracking Technologies: We use cookies and similar technologies to provide essential functionality like storing settings and recognizing you while using our Services.
- Non-essential Cookies: Depending on your jurisdiction, we may use online analytics products that use cookies to help us analyze how de-identified users use our Services and to enhance your experience when you use the Services. We may also employ third-party Cookies to gather data for interest-based advertising. In some jurisdictions, we only use non-essential cookies after obtaining your consent. See this section for more details and control options.

- Email Marketing Interactions: Our emails may have web beacons that offer information on your device type, email client, email reception, opens, and link clicks.
- Geolocation Information: Depending on the Service's functionality, we collect regional geolocation data.
- Service Usage Information: We collect data about your interactions with the Services, such as IP address, device information, session details, date and time of requests, device type and ID, operating system and application version, information related to your contributions to repositories, and performance of specific features or Services.
- Website Usage Data: We automatically log data about your Website interactions, including the referring site, date and time of visit, pages viewed, and links clicked.

From Third Parties

- Information from Other Users of the Services: Other users may share information about you when they submit issues and comments. We may also receive information about you if you are identified as a representative or administrator on your company's account.
- Publicly Available Sources: We may acquire information about you from publicly available sources like public GitHub repositories.
- Services you linked to your GitHub account: When you or your administrator integrate third-party apps or services with our Services, we receive information based on your settings with those services. This can include details like your name and email from services like Google for authentication. The information we receive depends on the third-party's settings and privacy policies. Always review these to understand what data is shared with our Services.
- Vendors, Partners, and Affiliates: We may receive information about you from third parties, like vendors, resellers, partners, or affiliates for the purposes outlined in this statement.

Processing Purposes: How We Use Your Personal Data

The Personal Data we process depends on your interaction and access methods with our Services, including the interfaces (web, desktop, mobile apps), features used (pull requests, Codespaces, GitHub Copilot), and your preferred access tools (like your IDE). This section details all the potential ways GitHub may process your Personal Data:

- Business Operations: We use Personal Data for activities like billing, accounting, and compensation. This includes creating aggregated statistical data for internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including product strategy).

- Communication: We use Personal Data to inform you about new Services, features, offers, promotions, and other pertinent information. This also includes sending confirmations, invoices, technical notices, updates, security alerts, and administrative messages.
- Inference: We generate new information from other data we collect to derive likely preferences or other characteristics. For instance, we infer your general geographic location based on your IP address.
- Personalization: We use Personal Data to customize the Service to your preferences, to evaluate the effectiveness of enterprise business ads and promotional communications, and to ensure a seamless and consistent user experience.
- Safety and Security: To promote safety, integrity, and security across our Services, we process Personal Data, using both automated and, at times, manual techniques for abuse detection, prevention, and violations of terms of service.
- Service Provision: We use Personal Data to deliver and update our Services as configured and used by You, and to make ongoing personalized experiences and recommendations.
- Troubleshooting: We use Personal Data to identify and resolve technical issues.
- Ongoing Service Performance: Personal Data helps us keep the Services up to date and performant, and meet user productivity, reliability, efficacy, quality, privacy, accessibility and security needs.
- Complying with and resolving legal obligations: including responding to Data Subject Requests for Personal Data processed by GitHub as Controller (for example website data), tax requirements, agreements and disputes.
- Delivering Professional Services: We use Personal Data to deliver training, consulting or implementation (“Professional Services”). This includes providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Improving Professional Services: Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying product(s) based on issues identified while providing Professional Services, including fixing software defects, and otherwise keeping the Professional Services up to date and performant.

When carrying out these activities, GitHub practices data minimization and uses the minimum amount of Personal Information required.

Sharing of Personal Data

We may share Personal Data with the following recipients:

- Abuse and Fraud Prevention Entities: We may disclose Personal Data based on a good faith belief it is needed to prevent fraud, abuse, or attacks on our Services, or to protect the safety of

GitHub and our users.

- Affiliates: Personal Data may be shared with GitHub affiliates, including Microsoft, to facilitate customer service, marketing and advertising, order fulfillment, billing, technical support, and legal and compliance obligations. Our affiliates may only use the Personal Data in a manner consistent with this Privacy Statement.
- GitHub Organization Accounts: If an organization adds you to their GitHub account, we might share Personal Data with that organization to fulfill the commercial relationship. In such a case, your use of the Services is protected by a data protection agreement and terms between your organization and GitHub
- Competent Authorities: We may disclose Personal Data to authorized law enforcement, regulators, courts, or other public authorities in response to lawful requests or to protect our rights and safety. Please refer to our Guidelines for Legal Requests of User Data for more information.
- Corporate Transaction Entities: we might disclose Personal Data within the limits of the law and in accordance with this Privacy Statement for strategic business transactions such as sales or a merger.
- Partners and Resellers: We cooperate with third-parties that offer sales, consulting, support, and technical services for our Services. We may share your data with these partners and resellers where allowed, and with your consent when required.
- Subprocessors and Service Providers: We may use vendors to provide services on our behalf, including hosting, marketing, advertising, social, analytics, support ticketing, credit card processing, or security services. They are bound by contractual obligations to ensure the security, privacy, and confidentiality of your information. Please visit https://docs.github.com/en/site-policy/privacy-policies/github-subprocessors to see our list of Subprocessors.
- Visual Studio Code (GitHub Codespaces): GitHub Codespaces and github.dev offer Visual Studio Code in a web browser, where some telemetry is collected by default. Details on telemetry collection are on the VS Code website. To opt out, go to File > Preferences > Settings in the top left menu of VS Code. Opting out will sync this preference across all future web sessions in GitHub Codespaces and github.dev.
- Other Third-party Applications: Upon your instruction, we may share Personal Data with third-party applications available on our Marketplace. You are responsible for the data you instruct us to share with these applications.
- Other Users and the Public: Depending on your account settings, we may share Personal Data with other users of the Services and the public. You control what information is made public. To adjust your settings, visit User Settings in your profile. Please be aware that any information you share in a collaborative context may become publicly accessible.

Private repositories: GitHub Access

If your GitHub account has private repositories, you control the access to that information. GitHub personnel does not access private repository information without your consent except as provided in this Privacy Statement and for:

- security purposes
- automated scanning or manual review for known vulnerabilities, active malware, or other content known to violate our Terms of Service
- to assist the repository owner with a support matter
- to maintain the integrity of the Services, or
- to comply with our legal obligations if we have reason to believe the contents are in violation of the law.

GitHub will provide you with notice regarding private repository access unless doing so is prohibited by law or if GitHub acted in response to a security threat or other risk to security.

Lawful Bases for Processing Personal Data (Applicable to EEA and UK End Users)

GitHub processes Personal Data in compliance with the GDPR, ensuring a lawful basis for each processing activity. The basis varies depending on the data type and the context, including how you access the services. Our processing activities typically fall under these lawful bases:

- Contractual Necessity: Processing is required to fulfill our contractual duties to you, in accordance with the GitHub Terms of Service.
- Legal Obligation: We process data when it's necessary to comply with applicable laws or to protect the rights, safety, and property of GitHub, our affiliates, users, or third parties.
- Legitimate Interests: We process data for purposes that are in our legitimate interests, such as securing our Services, communicating with you, and improving our Services. This is done only when these interests are not overridden by your data protection rights or your fundamental rights and freedoms.
- Consent: We process data when you have explicitly consented to such processing. When we rely on consent as the legal basis, you have the right to withdraw your consent for data processing at any time. The procedures for withdrawal are detailed in this Statement and available on our website.

Your Privacy Rights

Depending on your residence location, you may have specific legal rights regarding your Personal Data:

- The right to access the data collected about you
- The right to request detailed information about the specific types of Personal Data we've collected over the past 12 months, including data disclosed for business purposes
- The right to rectify or update inaccurate or incomplete Personal Data under certain circumstances
- The right to erase or limit the processing of your Personal Data under specific conditions
- The right to object to the processing of your Personal Data, as allowed by applicable law
- The right to withdraw consent, where processing is based on your consent
- The right to receive your collected Personal Data in a structured, commonly used, and machine-readable format to facilitate its transfer to another company, where technically feasible

To exercise these rights, please send an email to privacy[at]github[dot]com and follow the instructions provided. To verify your identity for security, we may request extra information before addressing your data-related request. Please contact our Data Protection Officer at dpo[at]github[dot]com for any feedback or concerns. Depending on your region, you have the right to complain to your local Data Protection Authority. European users can find authority contacts on the European Data Protection Board website, and UK users on the Information Commissioner's Office website.

We aim to promptly respond to requests in compliance with legal requirements. Please note that we may retain certain data as necessary for legal obligations or for establishing, exercising, or defending legal claims.

International data transfers

GitHub stores and processes Personal Data in a variety of locations, including your local region, the United States, and other countries where GitHub, its affiliates, subsidiaries, or subprocessors have operations. We transfer Personal Data from the European Union, the United Kingdom, and Switzerland to countries that the European Commission has not recognized as having an adequate level of data protection. When we engage in such transfers, we generally rely on the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, to help protect your rights and enable these protections to travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where GitHub processes personal data, see this article on the European Commission website.

Data Privacy Framework (DPF)

GitHub also complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. GitHub has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. GitHub has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy statement and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

GitHub has the responsibility for the processing of Personal Data it receives under the Data Privacy Framework (DPF) Principles and subsequently transfers to a third party acting as an agent on GitHub’s behalf. GitHub shall remain liable under the DPF Principles if its agent processes such Personal Data in a manner inconsistent with the DPF Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

Dispute resolution process

In compliance with the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF, GitHub commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU, UK, and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF, the UK Extension, and the Swiss-U.S. DPF should first contact GitHub at: dpo[at]github[dot]com.

If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://go.adr.org/dpf_irm.html for more information or to file a complaint. The services of the International Centre for Dispute Resolution are provided at no cost to you.

An individual has the possibility, under certain conditions, to invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms. For additional information visit https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2.

Government Enforcement

GitHub is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). Under Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), an organization's failure to abide by commitments to implement the DPF Principles may be challenged as deceptive by the FTC. The FTC has the power to prohibit such misrepresentations through administrative orders or by seeking court orders.

Security and Retention

GitHub uses appropriate administrative, technical, and physical security controls to protect your Personal Data. We'll retain your Personal Data as long as your account is active and as needed to fulfill contractual obligations, comply with legal requirements, resolve disputes, and enforce agreements. The retention duration depends on the purpose of data collection and any legal obligations.

Security

GitHub uses administrative, technical, and physical security controls where appropriate to protect your Personal Data.

Contact Us

Contact us via our contact form or by emailing our Data Protection Officer at dpo[at]github[dot]com. Our addresses are:

GitHub B.V. Prins Bernhardplein 200, Amsterdam 1097JB The Netherlands

GitHub, Inc. 88 Colin P. Kelly Jr. St. San Francisco, CA 94107 United States

Information for Minors

Our Services are not intended for individuals under the age of 13. We do not intentionally gather Personal Data from such individuals. If you become aware that a minor has provided us with

Personal Data, please notify us.

Changes to Our Privacy Statement

GitHub may periodically revise this Privacy Statement. If there are material changes to the statement, we will provide at least 30 days prior notice by updating our website or sending an email to your primary email address associated with your GitHub account.

Translations

Below are translations of this document into other languages. In the event of any conflict, uncertainty, or apparent inconsistency between any of those versions and the English version, this English version is the controlling version.

French

Cliquez ici pour obtenir la version française: Déclaration de confidentialité de GitHub (PDF).

Other translations

For translations of this statement into other languages, please visit https://docs.github.com/ and select a language from the drop-down menu under “English.”

Our use of cookies and tracking technologies

Cookies and tracking technologies

GitHub uses cookies to provide, secure and improve our Service or to develop new features and functionality of our Service. For example, we use them to (i) keep you logged in, (ii) remember your preferences, (iii) identify your device for security and fraud purposes, including as needed to maintain the integrity of our Service, (iv) compile statistical reports, and (v) provide information and insight for future development of GitHub. We provide more information about cookies on GitHub that describes the cookies we set, the needs we have for those cookies, and the expiration of such cookies.

For Enterprise Marketing Pages, we may also use non-essential cookies to (i) gather information about enterprise users' interests and online activities to personalize their experiences, including by making the ads, content, recommendations, and marketing seen or received more relevant and (ii) serve and measure the effectiveness of targeted advertising and other marketing efforts. If you disable the non-essential cookies on the Enterprise Marketing Pages, the ads, content, and marketing you see may be less relevant.

Our emails to users may contain a pixel tag, which is a small, clear image that can tell us whether or not you have opened an email and what your IP address is. We use this pixel tag to make our email communications more effective and to make sure we are not sending you unwanted email.

The length of time a cookie will stay on your browser or device depends on whether it is a "persistent" or "session" cookie. Session cookies will only stay on your device until you stop browsing. Persistent cookies stay until they expire or are deleted. The expiration time or retention period applicable to persistent cookies depends on the purpose of the cookie collection and tool used. You may be able to delete cookie data. For more information, see GitHub General Privacy Statement.

What are cookies and similar technologies?

We use cookies and similar technologies, such as web beacons, local storage, and mobile analytics, to operate and provide our Services. When visiting Enterprise Marketing Pages, like resources.github.com, these and additional cookies, like advertising IDs, may be used for sales and marketing purposes.

Cookies are small text files stored by your browser on your device. A cookie can later be read when your browser connects to a web server in the same domain that placed the cookie. The text in a cookie contains a string of numbers and letters that may uniquely identify your device and can contain other information as well. This allows the web server to recognize your browser over time, each time it connects to that web server.

Web beacons are electronic images (also called "single-pixel" or "clear GIFs") that are contained within a website or email. When your browser opens a webpage or email that contains a web beacon, it automatically connects to the web server that hosts the image (typically operated by a third party). This allows that web server to log information about your device and to set and read its own cookies. In the same way, third-party content on our websites (such as embedded videos, plug-ins, or ads) results in your browser connecting to the third-party web server that hosts that content.

Mobile identifiers for analytics can be accessed and used by apps on mobile devices in much the same way that websites access and use cookies. When visiting Enterprise Marketing pages, like resources.github.com, on a mobile device these may allow us and our third-party analytics and advertising partners to collect data for sales and marketing purposes.

We may also use so-called “flash cookies” (also known as “Local Shared Objects” or “LSOs”) to collect and store information about your use of our Services. Flash cookies are commonly used for advertisements and videos.

How do we and our partners use cookies and similar technologies?

The GitHub Services use cookies and similar technologies for a variety of purposes, including to store your preferences and settings, enable you to sign-in, analyze how our Services perform, track your interaction with the Services, develop inferences, combat fraud, and fulfill other legitimate purposes. Some of these cookies and technologies may be provided by third parties, including service providers and advertising partners. For example, our analytics and advertising partners may use these technologies in our Services to collect personal information (such as the pages you visit, the links you click on, and similar usage information, identifiers, and device information) related to your online activities over time and across Services for various purposes, including targeted advertising. GitHub will place non-essential cookies on pages where we market products and services to enterprise customers, for example, on resources.github.com.

We and/or our partners also share the information we collect or infer with third parties for these purposes.

The table below provides additional information about how we use different types of cookies:

Purpose	Description
Required Cookies	GitHub uses required cookies to perform essential website functions and to provide the services. For example, cookies are used to log you in, save your language preferences, provide a shopping cart experience, improve performance, route traffic between web servers, detect the size of your screen, determine page load times, improve user experience, and for audience measurement. These cookies are necessary for our websites to work.
Analytics	We allow third parties to use analytics cookies to understand how you use our websites so we can make them better. For example, cookies are used to gather information about the pages you visit and how many clicks you need to accomplish a task. We also use some analytics cookies to provide personalized advertising.

Purpose	Description
Social Media	GitHub and third parties use social media cookies to show you ads and content based on your social media profiles and activity on GitHub’s websites. This ensures that the ads and content you see on our websites and on social media will better reflect your interests. This also enables third parties to develop and improve their products, which they may use on websites that are not owned or operated by GitHub.
Advertising	In addition, GitHub and third parties use advertising cookies to show you new ads based on ads you've already seen. Cookies also track which ads you click or purchases you make after clicking an ad. This is done both for payment purposes and to show you ads that are more relevant to you. For example, cookies are used to detect when you click an ad and to show you ads based on your social media interests and website browsing history.

What are your cookie choices and controls?

You have several options to disable non-essential cookies:

1. **Specifically on GitHub Enterprise Marketing Pages**

   Any GitHub page that serves non-essential cookies will have a link in the page’s footer to cookie settings. You can express your preferences at any time by clicking on that linking and updating your settings.

   Some users will also be able to manage non-essential cookies via a cookie consent banner, including the options to accept, manage, and reject all non-essential cookies.

2. **Generally for all websites** You can control the cookies you encounter on the web using a variety of widely-available tools. For example:

- If your browser sends a Do Not Track (DNT) signal, GitHub will not set non-essential cookies and will not load third party resources which set non-essential cookies.
- Many browsers provide cookie controls which may limit the types of cookies you encounter online. Check out the documentation for your browser to learn more.
- If you enable a browser extension designed to block tracking, such as Privacy Badger, non-essential cookies set by a website or third parties may be disabled.

- If you enable a browser extension designed to block unwanted content, such as uBlock Origin, non-essential cookies will be disabled to the extent that content that sets non-essential cookies will be blocked.
- You may use the Global Privacy Control (GPC) to communicate your privacy preferences. If GitHub detects the GPC signal from your device, GitHub will not share your data (we do not sell your data). To learn more, visit Global Privacy Control — Take Control Of Your Privacy
- Advertising controls. Our advertising partners may participate in associations that provide simple ways to opt out of ad targeting, which you can access at:
- United States: NAI and DAA
- Canada: Digital Advertising Alliance of Canada
- Europe: European Digital Advertising Alliance

These choices are specific to the browser you are using. If you access our Services from other devices or browsers, take these actions from those systems to ensure your choices apply to the data collected when you use those systems.

US State Specific Information

This section provides extra information specifically for residents of certain US states that have distinct data privacy laws and regulations. These laws may grant specific rights to residents of these states when the laws come into effect. This section uses the term “personal information” as an equivalent to the term “Personal Data.”

Privacy Rights

These rights are common to the US State privacy laws:

- Right to Knowledge and Correction: You have the right to request details on the specific personal information we’ve collected about you and the right to correct inaccurate information. You can exercise this right by contacting us. You can also access and edit basic account information in your settings.
- Right to Know Data Recipients: We share your information with service providers for legitimate business operations, such as data storage and hosting. For more details, please see “Sharing Your Information” below.
- Right to request Deletion: You reserve the right to request the deletion of your data, barring a few exceptions. Such exceptions include circumstances where we are required to retain data to comply with legal obligations, detect fraudulent activity, investigate reports of abuse or other violations of our Terms of Service, or rectify security issues. Upon receiving your verified request,

we will promptly delete your personal information (unless an exception applies), and instruct our service providers to do the same. We employ brief retention terms by design.

- Right to a Timely Response: You are allowed to make two free requests in any 12-month period. We commit to responding to your request within 45 days. In complex cases, we may extend our response time by an additional 45 days.
- Non-Discrimination: We will not hold it against you when you exercise any of your rights. On the contrary, we encourage you to review your privacy settings closely and contact us with any questions.

Notice of Collection of Personal Information

We may collect various categories of personal information about our website visitors and users of "Services" which includes GitHub applications, software, products, or services. That information includes identifiers/contact information, demographic information, payment information, commercial information, internet or electronic network activity information, geolocation data, audio, electronic, visual, or similar information, and inferences drawn from such information.

We collect this information for various purposes. This includes identifying accessibility gaps and offering targeted support, fostering diversity and representation, providing services, troubleshooting, conducting business operations such as billing and security, improving products and supporting research, communicating important information, ensuring personalized experiences, and promoting safety and security.

Exercising your Privacy Rights

To make an access, deletion, correction, or opt-out request, please send an email to privacy[at]github[dot]com and follow the instructions provided. We may need to verify your identity before processing your request. If you choose to use an authorized agent to submit a request on your behalf, please ensure they have your signed permission or power of attorney as required.

To opt out of the sharing of your personal information, you can click on the "Do Not Share My Personal Information" link on the footer of our Websites or use the Global Privacy Control ("GPC") if available. Authorized agents can also submit opt-out requests on your behalf.

California

Mandatory Disclosures

We also make the following disclosures for purposes of compliance with California privacy law:

- We collected the following categories of personal information in the last 12 months: identifiers/contact information, demographic information (such as gender), payment card information associated with you, commercial information, Internet or other electronic network activity information, geolocation data, audio, electronic, visual or similar information, and inferences drawn from the above.
- The sources of personal information from whom we collected are: directly from you, automatically or from third parties.
- The business or commercial purposes of collecting personal information are as summarized above and in our Privacy Statement under Processing Purposes.
- We disclosed the following categories of personal information for a business purpose in the last 12 months: identifiers/contact information, demographic information (such as gender and rough geographic location), payment information, commercial information, Internet or other electronic network activity information, geolocation data, audio, electronic, visual or similar information, and inferences drawn from the above. We disclosed each category to third-party business partners and service providers, third-party sites or platforms such as social networking sites, and other third parties as described in the Sharing of Personal Data section of our Privacy Statement.
- As defined by applicable law, we “shared” the following categories of personal information in the last 12 months: identifiers/contact information, Internet or other electronic network activity information, and inferences drawn from the above. We shared each category to or with advertising networks, data analytics providers, and social networks.
- The business or commercial purpose of sharing personal information is to assist us with marketing, advertising, and audience measurement.
- We do not “sell” or “share” the personal information of known minors under 16 years of age.

Shine the Light Act

Under California Civil Code section 1798.83, also known as the “Shine the Light” law, California residents who have provided personal information to a business with which the individual has established a business relationship for personal, family, or household purposes (“California Customers”) may request information about whether the business has disclosed personal information to any third parties for the third parties’ direct marketing purposes. Please be aware that we do not disclose personal information to any third parties for their direct marketing purposes as defined by this law. California Customers may request further information about our compliance with this law by emailing (privacy[at]github[dot]com). Please note that businesses are required to respond to one request per California Customer each year and may not be required to respond to requests made by means other than through the designated email address.

Removal of Content

California residents under the age of 18 who are registered users of online sites, services, or applications have a right under California Business and Professions Code Section 22581 to remove, or request and obtain removal of, content or information they have publicly posted. To remove content or information you have publicly posted, please submit a Private Information Removal request. Alternatively, to request that we remove such content or information, please send a detailed description of the specific content or information you wish to have removed to GitHub support. Please be aware that your request does not guarantee complete or comprehensive removal of content or information posted online and that the law may not permit or require removal in certain circumstances. If you have any questions about our privacy practices with respect to California residents, please send an email to privacy[at]github[dot]com.

We value the trust you place in us and are committed to handling your personal information with care and respect. If you have any questions or concerns about our privacy practices, please email our Data Protection Officer at dpo[at]github[dot]com.

Colorado/Connecticut/Virginia

If you live in Colorado, Connecticut, or Virginia you have some additional rights:

- If we deny your rights request, you have the right to appeal that decision. We will provide you with the necessary information to submit an appeal at that time.
- You have the right to opt out of profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer. GitHub does not engage in such profiling as defined by Colorado law, so there’s no need to opt out.

Nevada

We do not sell your covered information, as defined under Chapter 603A of the Nevada Revised Statutes. If you still have questions about your covered information or anything else in our Privacy Statement, please send an email to privacy[at]github[dot]com.

Legal

Terms Privacy Status Pricing Expert services Blog